AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method for limiting the impact of undesirable behavior of computers on a network through which packets of data are interchanged between the computers, comprising:

monitoring the network for any patterns of behavior;

determining, upon discovering that one or more of the patterns of behavior is undesirable, a type of the undesirable pattern of behavior;

determining a proper action for mitigating that type of undesirable behavior, the proper action including preventing dissemination through the network of packets associated with the undesirable behavior and allowing dissemination of packets not associated with the undesirable behavior,

wherein preventing dissemination comprises at least one of changing a routing table, changing a forwarding table, turning off at least one port of a forwarding device, filtering on Internet Protocol (IP) addresses, and filtering on media access control (MAC) addresses.

2. (Original) The method of claim 1, wherein a discovery, including that of a network topology, facilitates the network monitoring and type of undesirable behavior determination.

3. (Original) The method of claim 1, wherein the dissemination through the network of packets associated with the undesirable behavior is prevented for a time period that is lengthened gradually as long as the undesirable behavior continues or intermittently reappears, the time period being gradually shortened if the undesirable behavior stops for a predetermined time.

4. (Original) The method of claim 3, wherein the time period corresponds to a skepticism level that depends on a history of the undesirable pattern of behavior, a skepticism level zero (0) denoting a good history.

5. (Original) The method of claim 1, wherein the undesirable pattern of behavior is characterized in that it matches behavior defined by a network administrator as notable or undesirable.

6. (Original) The method of claim 1, wherein the undesirable pattern of behavior is any network pathology characterized as a broadcast storm or an address resolution protocol (ARP) fight.

7. (Original) The method of claim 1, wherein the undesirable pattern of behavior includes any one or more of a stolen Internet protocol (IP) address, a stolen media access control (MAC) address, a malformed packet, too many packets directed to an overloaded server, too many probe packets directed to a firewall or too many ARP request packets.

8. (Currently Amended) The method of claim [[1]] 59, wherein preventing the dissemination of the undesirable pattern of behavior includes discarding the packets associated with such behavior, isolating any of the computers at which such behavior originates, or isolating any network segments at which such behavior originates.

9. (Original) The method of claim 1, wherein the undesirable pattern of behavior is a broadcast storm, and wherein the monitoring includes

recovering a topology of the network using information obtained through a network management protocol interface, and

learning historical packet traffic statistics for any segment of the network.

10. (Original) The method of claim 9, wherein the network management protocol is the simple network management protocol (SNMP).

11. (Original) The method of claim 1, wherein the undesirable pattern of behavior is a broadcast storm, and wherein the monitoring includes learning a topology of the network from a forwarding database or table of a forwarding device in the network.

12. (Original) The method of the claim 1, wherein the network is a shared data network.

13. (Original) The method of claim 11, wherein the network is a switched Ethernet network and the forwarding device is a switch.

14. (Original) The method of claim 11, wherein the network is a bridged Ethernet network and the forwarding device is a bridge or a smart bridge.

15. (Original) The method of the claim 1, wherein the undesirable pattern of behavior is too many ARP requests and wherein the monitoring includes verifying stability and lack of conflicts in an IP or MAC address mapping.

16. (Currently Amended) The method of the claim 1, wherein the proper action <u>further</u> includes alerting a system administrator about the existence of the undesirable pattern of behavior.

17. (Original) The method of claim 1, wherein the undesirable pattern of behavior is a simultaneous use of a network address, and wherein the proper action includes disabling any address associated to the network address that contradicts an address list in a network server or disabling any associated address that is not included in a list of addresses that are allowed to map to the network address.

18. (Original) The method of claim 1, wherein, if available from any one of the computers, the monitored pattern of behavior further includes information about a pattern of behavior by another one of the computers, the method further comprising:

determining if the information about the pattern of behavior is trustworthy.

19. (Original) The method of claim 18, wherein filters and network configuration parameters are used in determining the trustworthiness.

20. (Original) The method of claim 2, wherein understanding the network topology facilitates disablement of ports in forwarding devices that connect to offending computers.

21. (Original) The method of claim 3 wherein the time period becomes longer in a random exponential backoff before an attempt is made to allow resumption of the packets from any offending computer that originated the undesirable pattern of behavior, the time period becoming longer if the undesirable pattern of behavior reoccurs during a current backoff time, the time period becoming shorter if the undesirable pattern of behavior disappears and does not reoccur in the current backoff time.

22. (Currently Amended) A system for limiting the impact of undesirable behavior of computers on a network through which packets of data are interchanged between the computers, comprising:

means for monitoring the packets for any patterns of behavior;

means for determining, upon discovering that one or more of the patterns of behavior is undesirable, a type of the undesirable pattern of behavior;

means for determining a proper action for mitigating that type of undesirable behavior, the proper action, performed by mitigation means, including preventing dissemination through the network of packets associated with the undesirable behavior and allowing dissemination of packets not associated with the undesirable behavior,

wherein preventing dissemination comprises at least one of changing a routing table, changing a forwarding table, and turning off at least one port of a forwarding device.

23. (Original) The system of claim 22, wherein means for discovery, including that of a network topology, facilitates network monitoring and type of undesirable behavior determination.

24. (Currently Amended) The ~~method~~ system of claim [[1]] 22, wherein the dissemination through the network of packets associated with the undesirable behavior is prevented for a time period that is lengthened gradually as long as the undesirable behavior continues or intermittently reappears, the time period being gradually shortened if the undesirable behavior stops for a predetermined time.

25. (Currently Amended) The system of claim [[22]] 24, wherein the time period corresponds to a skepticism level that depends on a history of the undesirable pattern of behavior, a skepticism level zero (0) denoting a good history.

26. (Original) The system of claim 22, wherein the undesirable pattern of behavior is characterized in that it matches behavior defined by a network administrator as notable or undesirable.

27. (Original) The system of claim 22, wherein the undesirable pattern of behavior is any network pathology characterized as a broadcast storm or an address resolution protocol (ARP) fight.

28. (Original) The system of claim 22, wherein the undesirable pattern of behavior includes any one or more of a stolen Internet protocol (IP) address, a stolen media access control (MAC) address, a malformed packet, too many packets directed to an overloaded server, too many probe packets directed to a firewall or too many ARP request packets.

29. (Original) The system of claim 22, wherein preventing the dissemination of the undesirable pattern of behavior includes discarding the packets associated with such behavior, isolating any of the computers at which such behavior originates, or isolating any network segments at which such behavior originates.

30. (Original) The system of claim 22, wherein the undesirable pattern of behavior is a broadcast storm, and wherein the monitoring means includes

means for recovering a topology of the network using information obtained through a standard SNMP (simple network management protocol) interface, and

means for learning historical packet traffic statistics for any segment of the network.

31. (Original) The system of claim 23, wherein the undesirable pattern of behavior is a broadcast storm, and wherein the monitoring means includes means for learning the topology of the network from a forwarding database or table of a forwarding device in the network.

32. (Original) The system of claim 31, wherein the network is a switched Ethernet network and the forwarding device is a switch.

33. (Original) The system of claim 22, wherein the network is a shared data network.

34. (Original) The system of claim 22, wherein the undesirable pattern of behavior is too many ARP requests and wherein the monitoring means includes means for verifying stability and lack of conflicts in an IP or MAC address mapping.

35. (Original) The system of claim 22 wherein the proper action includes alerting a system administrator about the existence of the undesirable pattern of behavior.

36. (Original) The system of claim 22, wherein the undesirable pattern of behavior is a simultaneous use of a network address, and wherein the proper action includes disabling any address associated to the network address that contradicts an address list in a network server or disabling any associated address that is not included in a list of addresses that are allowed to map to the network address.

37. (Original) The system of claim 22, wherein, if available from any one of the computers, the monitored pattern of behavior further includes information about a pattern of behavior by another one of the computers, the method further comprising:

determining if the information about the pattern of behavior is trustworthy.

38. (Original) The method of claim 37, wherein filters and network configuration parameters are used in determining the trustworthiness.

39. (Original) The method of claim 23, wherein understanding the network topology facilitates disablement of ports in forwarding devices that connect to offending computers.

40. (Currently Amended) The system of claim [[22]] 24 wherein the time period becomes longer in a random exponential backoff before an attempt is made to allow resumption of the packets from any offending computer that originated the undesirable pattern of behavior, the time period becoming longer if the undesirable pattern of behavior reoccurs during a current backoff time, the time period becoming shorter if the undesirable pattern of behavior disappears and does not reoccur in the current backoff time.

41. (Cancelled)

42. (Original) A system for limiting the impact of undesirable behavior of computers on a network through which packets of data are interchanged between the computers, comprising:

one or more forwarding devices; and

one or more packet traffic monitors each including

means for monitoring the network for any patterns of behavior, including, if available, information about a pattern of behavior from any of the computers about another one of the computers;

means for determining if the information about the pattern of behavior from any of the computers is trustworthy;

means for determining, upon discovering that one or more of the patterns of behavior is undesirable, a type of the undesirable pattern of behavior;

means for determining a proper action for mitigating that type of undesirable behavior, the proper action, performed by mitigation means controlling the one or more forwarding devices, including preventing dissemination through the network of packets associated with the undesirable behavior and allowing dissemination of packets not associated with the undesirable behavior.

43. (Original) The method of claim 42, wherein means for discovery, including that of the network topology, facilitates network monitoring and type of undesirable behavior determination.

44. (Currently Amended) The method of claim 42, wherein the dissemination through the network of packets associated with the undesirable behavior is prevented for a time period that is exponentially increasing ~~exceeding~~ as long as the undesirable behavior continues or intermittently reappears, the time period being exponentially shortened if the undesirable behavior stops for a predetermined time.

45. (Original) The system of claim 42, wherein the packet traffic monitor is a separate device connected to the network and through the network to the one or more forwarding devices.

46. (Original) The system of claim 42, wherein one or more of the computers have a dedicated built-in packet traffic monitor.

47. (Original) The system of claim 42, wherein one or more of the forwarding devices have a dedicated built-in packet traffic monitor.

48. (Original) The system of claim 42, wherein the network is a switched Ethernet network and forwarding devices are switches.

49. (Original) The system of claim 42, wherein the one or more forwarding devices include any combination of zero or more switches and routers.

50. (Original) The system of claim 42, wherein the network is a bridged network and the forwarding devices are bridges or smart bridges.

51. (Original) The system of claim 42, wherein the one or more packet traffic monitors are placed in a strategic location of the network that is intended to maximize the packet traffic monitor's effectiveness in monitoring and mitigating the patterns of undesirable behavior, the strategic locations including one or more locations characterized as being next to an originator of the that behavior, at or next to each computer, at or next to each forwarding device or at the segment where the packets are to be monitored.

52. (Original) The system of claim 42, wherein the one or more packet traffic monitors is placed in a strategic location of the network that is intended to maximize the packet traffic monitor's effectiveness in monitoring and mitigating the patterns of undesirable behavior, the strategic locations including a high-speed network segment.

53. (Original) The system of claim 42, wherein the one or more packet traffic monitors is placed in a strategic location of the network that is intended to maximize the packet traffic monitor's effectiveness in monitoring and mitigating the patterns of undesirable behavior, the strategic locations including a place next to or at a network server.

54. (Original) The system of claim 42, wherein the one or more packet traffic monitors is implemented as a software module.

55. (Original) The system of claim 42, wherein the software module is a part of an operating system.

56. (Original) The system of claim 42, wherein the software module is a privileged application.

57. (Original) The system of claim 42, wherein the one or more packet traffic monitors co-operate with one another in the discovery of the patterns of behavior.

58. (Original) The system of claim 42, wherein the one or more packet traffic monitors are configured to sample points on the network randomly or selectively rather than sampling the entire network.

59. (New) A method comprising:

monitoring a network for an undesirable pattern comprising at least one of a stolen Internet Protocol (IP) address, a stolen media access control (MAC) address, a malformed packet, too many probe packets directed to a firewall, and too many address resolution protocol (ARP) packets;

determining a type of the undesirable pattern; and

determining an action to mitigate the undesirable pattern based on the type of undesirable behavior, the action comprising preventing dissemination over the network of packets associated with the undesirable pattern.

60. (New) The method of claim 59, wherein preventing the dissemination is performed for a period of time, the method further comprising:

lengthening the period of time as long as the undesirable behavior continues or intermittently reappears; and

shortening the period of time in response to the undesirable behavior stopping for at least a predetermined time.

61. (New) A system comprising:

a network interface to a network; and

a packet traffic monitor to:

monitor the network for an undesirable behavior;

determine a type of the undesirable behavior;

discover a topology of the network; and

cause prevention of dissemination over the network of packets associated with the undesirable behavior based on the type of the undesirable behavior and topology of the network.

62. (New) The system of claim 61, wherein the packet traffic monitor discovers the topology of the network by discovering that the network is one of a router-based network, a bridge-based network, and a switch-based network.

63. (New) The system of claim 61, wherein prevention of dissemination comprises at least one of changing a routing table, changing a forwarding table, turning off a port of a forwarding device, filtering on an Internet Protocol (IP) address, and filtering on a media access control (MAC) address.